AMENDMENTS TO THE SPECIFICAIION

Please replace paragraph beginning at line 17 of page 2, as follows:

A1

In cyberspace, where an agreement may exist in electronic form (i.e., electronic chattel paper), it is difficult to determine who has possession of an electronic chattel paper. It is an easy task for a party to create an identical copy of an electronic file and distribute that copy to others. In this situation, it appears impossible to identify which copy of the file is original, and thus, to identify who has possession of the original. However, from a legal perspective, it is necessary to be able to distinguish an original electronic chattel from a copy. Thus, there is a need in the art for a technique to maintain an original authoritative copy of an electronic chattel paper and to distinguish it from copies.

Please replace the paragraph beginning at line 1 of page 15, as follows:

A2

The Client Program 215 encrypts the final documents prior to storing them on the client 210. The input to the encryption process includes the unencrypted final documents and a document encryption key. The Client Program 215 generates the document encryption key based on a proprietary algorithm and a proprietary set of data. Those skilled in the art will understand that a variety of techniques may be used to generate a secure encryption key and it is not necessary to disclose the proprietary algorithm used by MBCC to enable the present invention. The Client Program 215 also generates an encryption key to be used for encrypting one or more signature files ("Signature Key"). The signature files contain digital representations of the signatures of various parties. The Signature Key is based, at least in part, on the contents of the unencrypted final documents. Basing the Signature Key on the unencrypted final documents ~~the~~ prevents creation of fraudulent final documents. For instance, if the final documents are modified, then the Credit Highway can no longer generate the Signature Key. As a result, the Credit Highway can also no longer decrypt the signature files. Thus, the signature files become invalid if a party modifies the final documents.

Please replace the paragraph beginning at line 23 of page 20, as follows:

A3

After the Electronic Agreement has been transferred to the server 110, the only authoritative copy of the Electronic Agreement is maintained on the database 120. Access to the Electronic Agreement is restricted to authorized users. The present invention anticipates several techniques to satisfy the recommendations of the proposed UCC revisions. In one embodiment, the authoritative copy of the Electronic Agreement includes a special header or text field that is encrypted with a separate encryption key. Any hard copies or electronic copies of the Electronic Agreement generated or created from the MB Advantage System will contain this special header ~~of~~ or field in its encrypted state. Thus, these copies can be distinguished from the authoritative copy. In another embodiment, the MB Advantage System will add a notice to each printed or viewed copy of the Electronic Agreement indicating that the copy is not the authoritative copy of the Electronic Agreement. In yet another embodiment, the MB Advantage System maintains at all times the location of the authoritative copy of the Electronic Agreement by recording the user creating the document or the user that checked out the document last. In this embodiment, the Server Software 115 maintains the identity of the authoritative copy of the Electronic Agreement.